Remarks

The above Amendments and these Remarks are in reply to the Office Action mailed August 28, 2006. A Petition for Extension of Time is submitted herewith, together with the appropriate fee.

I. Summary of Examiner's Rejections

Prior to the Office Action mailed August 28, 2006, Claims 1-9 and 21-31 were pending in the Application. In the Office Action, Claims 1-2, 5, 7-8, 21-22, 24, 26-27 and 29-31 were rejected under 35 U.S.C. 103(a) as being obvious over Brownlie et al. (U.S. Patent No. 6,202,157, hereinafter Brownlie) in view of Donohue (U.S. Patent No. 6,199,204). Claim 6 was rejected under 35 U.S.C. 103(a) as being unpatentable over Brownlie in view of Donohue and further in view of Wang (U.S. Patent No. 5,956,521). Claims 3-4 and 9 were rejected under 35 U.S.C. 103(a) as being unpatentable over Brownlie in view of Donohue and further in view of TRCKA et al. (U.S. Publication No. 2001/0039579) and Microsoft Press (Computer Dictionary, 3rd Edition, ISBN:157231446XA, 1997).

II. Summary of Applicant's Amendment

The present Response amends Claims 1, 7, 21, 26, 30 and 31, leaving for the Examiner's present consideration Claims 1-9 and 21-31. Reconsideration of the Application, as amended, is respectfully requested. Applicant respectfully reserves the right to prosecute any originally presented or canceled claims in a continuing or future application.

III. Claim Rejections under 35 U.S.C. § 103(a)

In the Office Action mailed August 28, 2006, Claims 1-2, 5, 7-8, 21-22, 24, 26-27 and 29-31 were rejected under 35 U.S.C. 103(a) as being obvious over Brownlie et al. (U.S. Patent No. 6,202,157, hereinafter Brownlie) in view of Donohue (U.S. Patent No. 6,199,204).

Claim 1

Claim 1 has been amended to more clearly define the embodiment therein. As amended, Claim 1 defines:

> *1. A system for maintaining security in a distributed computing environment, comprising:*
> *(1) a policy manager, coupled to a network, including*

a database for storing a security policy including a plurality of rules that control user access to applications; and

a policy distributor, coupled to the database, for distributing the plurality of rules through the network;

(2) a security engine located on a client coupled to the network, for storing a set of the plurality of rules constituting a local customized security policy received through the network from the policy distributor, and for enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

(3) an application, coupled to the security engine;

wherein the security policy is updated by keeping track of a series of incremental changes to the security policy, computing an accumulated delta that reflects the series of incremental changes and sending the accumulated delta to the security engine from the policy manager such that the security engine uses the delta to update the local customized security policy.

Claim 1 defines a system for maintaining security in a distributed computing environment that includes a policy manager, a security engine and an application coupled to the security engine. A security policy is stored in a database and this policy includes a plurality of rules that control user access to applications. The security engine located at the client enforces the local policy of that client by evaluating the rules of the local policy upon receiving an access request to the application and grants or denies access based on that evaluation. Furthermore, updates to the security policy are performed by keeping track of incremental changes, computing an accumulated delta and sending the accumulated delta to the security engine from the policy manager where it can be used to update the local custom policy.

The advantages of the features of Claim 1 include for example, the ability for a local security engine to control (grant or deny) access to applications by evaluating a subset of rules distributed from a central source. The rules which control the access can be matched to access requests and can be specific for a local client. Furthermore, accumulating incremental changes and distributing the accumulated delta allows more efficient updates to the local security policy when many rules of the policy are being continuously updated by various users or applications.

Brownlie teaches computer network security system and method having unilateral enforceable security policy provision. More particularly, Brownlie appears to disclose a central server that provides security policy parameters to network nodes. Such parameters include policies related to password aging, length of password, allowed cryptographic algorithms, length of keys, lifetime rules related to certificates, etc. (col. 3, lines 25-44). Thus, Brownlie appears to

disclose the distribution of security policy rule data that specifies administrative parameters of network security.

Donohue, on the other hand, teaches distribution of software updates via a computer network. More particularly, Donohue appears to disclose an updater agent that accesses relevant network locations and automatically downloads and installs available updates to a software program (Donohue, Abstract). However, Applicant respectfully submits that Brownlie in combination with Donohue fail to disclose the features of Claim 1.

Firstly, Brownlie in combination with Donohue fail to disclose updating a security policy by keeping track of a series of incremental changes to the security policy, computing an accumulated delta that reflects the series of incremental changes and sending the accumulated delta to the security engine from the policy manager such that the security engine uses the delta to update the local customized security policy, as defined in Claim 1. Brownlie is not concerned with updating the security policy in such a manner. Donohue, on the other hand appears to disclose distribution of software updates by providing patch code and installation instructions online (col. 7, line 59 – col. 8, line 11). Further, Donohue teaches an updater component that decides which version to upgrade to (such as the highest possible version) and performs various steps to bring the current application to the new level (col. 9, lines 44-59). However, such distribution of software patches is not the same as *updating a security policy* by keeping track of incremental changes to a security policy, computing an accumulated delta and sending that delta to the client from the policy manager, as defined in Claim 1. Neither Donohue nor Brownlie appear to keep track of any incremental changes to a security policy. Similarly, neither Donohue nor Brownlie appear to compute an accumulated delta that reflects these changes. In fact, Donohue does not appear to be at all concerned with updating any security policy on the network. Installing new versions of computer software programs is not the same as these features of Claim 1.

Furthermore, in the Office Action, it was proposed that these features are merely an obvious variation of possible security change implementations (Office Action, page 5). Applicant respectfully disagrees. Claim 1 defines a security policy that is comprised of a plurality of rules that control access to various applications. This plurality of rules can include hundreds or thousands of access rules which are constantly being updated and modified by various users or applications (par. [0093]). For example any single change can include adding rules, deleting rules or amending rules, renaming users, etc. (par. 0095]). By keeping track of incremental changes, accumulating a delta and sending that delta to the client by the policy distributor, the

local policy is able to be more efficiently updated, as defined in Claim 1. For example, various ongoing changes can offset each other, such as when a rule is added into one incremental change and later deleted from another incremental change, etc. (par. [0095]). Network traffic is reduced by pre-computing and distributing only accumulated changes to the security policy (par. [0096]). Furthermore, the security policy can be easily rolled back to a previously enforced version by using this delta (p. [0106]).

Thus, Claim 1 clearly defines various advantageous features which are not disclosed in any of the cited references. As such, any modification to these references as proposed in the Office Action (page 5) must be drawn from impermissible hindsight. Accordingly, Applicant respectfully requests reconsideration of this rejection.

Secondly, Brownlie in combination with Donohue fail to disclose a distributed customized security policy that is enforced by matching a user access request to the plurality of rules of the policy and granting or denying access to a local application based on the match, as defined in Claim 1. Instead, Brownlie merely teaches that policy parameters are distributed to clients to be enforced thereon. These policy parameters relate to policies relating to password aging, password reuse, length of password, allowed cryptographic key lengths, etc. (col. 3, lines 25-49). These policy parameters thus appear to be mere administrative network security parameters and do not include a plurality of rules that are matched to an access request in order to control access to a local application, as defined in Claim 1. In other words, the policy rule data taught in Brownlie merely specifies various administrative security parameters that each node in the network should follow, while Claim 1 distributes the actual access/deny rules which are evaluated by matching them to an access request in order to grant or refuse access to a local application. Similarly, Donohue does not appear to be at all concerned with such a distributed security policy that controls access to various applications.

In view of the above comments, Applicant respectfully submits that Claim 1, as amended, is neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

Claims 7, 21, 26, 30 and 31

Claims 7, 21, 26, 30 and 31, while independently patentable, recite limitations that, similarly to those described above with respect to Claim 1, are not taught, suggested nor

otherwise rendered obvious by the cited references. Reconsideration thereof is respectfully requested.

Claims 2-6, 8-9, 22-25 and 27-29

Claims 2-6, 8-9, 22-25 and 27-29 are not addressed separately, but it is respectfully submitted that these claims are allowable as depending from an allowable independent claim, and further in view of the comments provided above. Applicant respectfully submits that Claims 2-6, 8-9, 22-25 and 27-29 are similarly neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

It is also submitted that these claims also add their own limitations which render them patentable in their own right. Applicant respectfully reserves the right to argue these limitations should it become necessary in the future.

IV. Conclusion

In view of the above amendments and remarks, it is respectfully submitted that all of the claims now pending in the subject patent application should be allowable, and reconsideration thereof is respectfully requested. The Examiner is respectfully requested to telephone the undersigned if he can assist in any way in expediting issuance of a patent.

Enclosed is a PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.136 for extending the time to respond up to and including December 28, 2006.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 06-1325 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: December 27, 2006

By: /Justas Geringson/

Justas Geringson
Reg. No. 57,033

Customer No.: 23910
FLIESLER MEYER LLP
650 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 362-3800
Fax: (415) 362-2928